- PATENT -

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPELLANTS:	Banks, Robert et al.	EXAMINER:	Jackson, J.
SERIAL NO.:	09/597,315	GROUP:	2131
FILED:	June 20, 2000	CASE NO.:	CE08314R
TITLED:	Method and Apparatus for Interfacing A Network to an External Network		

Motorola, Inc.
Corporate Offices
1303 E. Algonquin Road
Schaumburg, IL 60196
July 11, 2006

APPEAL BRIEF UNDER 37 CFR 41.37

Mail Stop Appeal Brief - Patents
Commissioner of Patents
P.O. Box 1450
Alexandria, Va. 22313-1450

Commissioner:

The Appellants hereby respectfully submit the following Appeal Brief in response to a Final Office Action dated November 29, 2007 and a Notice of Appeal filed March 31, 2008.

1. REAL PARTY IN INTEREST

The real party in interest in this appeal is Motorola, Inc.

2. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal.

3. STATUS OF CLAIMS

The status of the claims in the proceeding is:

1. Claims 1-12 and 14-38 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over United States Patent No. 6,012,100 to Frailong et al. in view of United States patent No. 6,285,667 to Willars et al.
2. Claims 13 is cancelled.

Claims 1-12 and 14-38 are hereby appealed.

4. STATUS OF AMENDMENTS

A Final Office Action mailed on November 29, 2007 and is currently pending. No post-final amendments were made to the claims in response to the Final Office Action was sent. The Appellant filed a Notice of Appeal on March 31, 2008.

5. SUMMARY OF CLAIMED SUBJECT MATTER

A services delivery element (26) forms an interface between an external element (such as an external end user's network feature server) and a communication network including both a core network (10) and an access network (12). The services delivery element (26) provides access to the core network (10) and access networks (12) to which the external element is interfaced. See Abstract.

Claim 1, as amended, provides for an apparatus (26) that interfaces a communication network (10) to a feature server (22, 23, 24) that is external to the network. The apparatus comprises a service delivery element (26) that is within the communication network (10). The service delivery element comprises (a) at least one internal interface to couple the service delivery element to other devices within the communication network; (b) an external interface to couple the service delivery element to at least one feature server external to the communication network; (c) an embedded security layer (302, 408) to authenticate the at least one feature server on the communication network and to provide a secure interface for the at least one feature server to the communication network through the external interface and (d) a processor adapted to operate responsive to a control program stored within a memory associated with the processor. The service delivery element operates to recognize the feature server, to negotiate a security level between the feature server and the communication network, and to manage access by the feature server to the communication network. See FIGs. 1, 3 and 4; page 3, lines 7-28, page 4, lines 11-24; page 5, lines 1-14, page 6, line 18 to page 7, line 8; page 8, lines 6 to page 9, line 12; page 13, lines 20-25, and claim 1.

Claim 22, as amended, provides a method of interfacing a communication network (10) to a feature server (22, 23, 24) that is external to the network. The claimed method comprises providing a service delivery element (26). The service delivery element is within the communication network and has an internal interface to couple the service delivery element to other elements within the communication network, an external interface to couple the service delivery element to the feature server external to the network and an embedded security layer (302, 408). The method also comprises recognizing the feature server via the service delivery element and authenticating the feature server for use on the communication network by the embedded security layer. Moreover, the method comprises providing a secure interface for the at least one feature server to the communication network through the external interface by way of the embedded security layer; negotiating a security level between the feature server and the

communication network, and metering access via the service delivery element by the feature server to the communication network in view of the security level. See FIGs. 1, 3 and 4; page 3, lines 7-28, page 4, lines 11-24; page 5, lines 1-14, page 6, line 18 to page 7, line 8; page 8, lines 6 to page 9, line 12; page 13, lines 20-25, and claim 22.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-12 and 14-38 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over United States Patent No. 6,012,100 to Frailong et al. in view of United States Patent No. 6,285,667 to Willars et al.

7. ARGUMENT

(i) Rejection under 35 U.S.C. §112, first paragraph:

None.

(ii) Rejection under 35 U.S.C. §112, second paragraph:

None.

(iii) Rejection under 35 U.S.C. §102:

None.

(iv) Rejection under 35 U.S.C. §103:

The present invention as found in independent claims 1 and 22 is directed to an apparatus and a method that interfaces a communication network to a feature server that is external to the network. The apparatus and method provides a service delivery element that is internal to the communication network. The service delivery element includes an internal interface to couple the service delivery element to other devices within the communication network as well as an external interface to couple the service delivery element to feature servers that are external to the communication network. An embedded

security layer is a part of the service delivery element and is provided for authenticating the feature server on the communication network and providing a secure interface for the feature server to the communication network through the external interface. The service delivery element recognizes the feature server, negotiates a security level between the feature server and the communication network, and manages access by the feature server to the communication network.

During the prosecution of this case, the claims were amended to clarify that the present invention provides a service delivery element for interfacing a feature server to a communication network. The service delivery element includes the internal interface, external interface and embedded security layer. The embedded security layer provides a secure interface at the external interface for the external feature service to the communication network. The service delivery element negotiates a security level between the feature server and the network and manages access of the external feature server to the communication network. Claims 1 and 22 are directed to controlling the interface between the feature server and the network by use of a service delivery element, thereby enabling a securing of the interface between the network and the feature server. The service delivery element thereby expands services available to a subscriber, such as an end user's computer, via the communication network.

As seen in the claims, the service delivery element is a part of the communications network and completely contained therein. It connects to other components of the communications network through an internal interface and connects to the feature server, which is external to the communications network, through the external interface. In addition, the security layer is embedded as a part of the service delivery element and authenticates the feature server for use on the communication network. The security layer is therefore completely within the communication network and provides a secure interface for which the communication network can have access to the feature server. Thus, the claim includes a service delivery element that is internal to the communication network, provides the security function within the communication network by negotiating a security level between the feature server and the

communication network and provides a secure interface between the communication network and the external feature server.

On the other hand, Frailong discloses a network interface device for connecting a client computer to an external network. The network interface device is configured for the client system by automated procedures and protocols initiated from a remote server. Software programs within the network interface device provide transparent communication between the client computer system and services available on the external network. Similar software programs and a configuration database within the network interface device provide transparent communication between the client computer system and the remote server.

In contrast to the present invention, Frailong teaches an interface for interfacing the client user itself, for example, a client computer network, and more particularly client personal computers of a LAN, to a communication network, in particular a WAN and more particularly the Internet. Frailong teaches an interface for connecting a computer system, to the Internet and more particularly for enabling the computer system to obtain a transport service for access to the Internet (see col. 2, lines 16-21). That is, Frailong merely teaches a configuring of an interface such as a subscriber/client gateway, to the Internet.

Frailong's gateway interface device is equated with the claimed service delivery element. Frailong's gateway interface device is in the client network and is not internal to the network such as the Internet. See FIG. 2. In addition, the Office Actions refer to the Secure Sockets Layer (SSL), column 18 lines 16-45, as teaching the embedded security layer and the security function found in the claims. As seen in this citation to Frailong, the SSL works with the gateway interface device and remote management server, which is separate from the gateway interface device and the client network, for teaching the security function found in the claims. With the combination of the gateway interface and the remote management server, Frailong disperses the functions of the claimed services delivery element into different devices where those devices are spread

between different networks so that the security can be provided. The SSL establishes the "trust relationship," e.g. security features, between the various elements external to the network to the network. As stated, amended claims 1 and 22 provide for a feature server being external to the network where the service delivery element that recognizes, negotiates security levels and manages access for the feature server into the communication network is internal to the communications device and contained within one device.

The fundamental difference between Frailong and the present invention as found in the amended claims is that Frailong is discussing the external element as an end user computer in a client Local Area Network and is concerned in providing access for that user computer in the Local Area Network to an external network. Frailong discloses the gateway interface device interacting between the LAN and the external communication network. On the other hand, the present invention discusses the service delivery element in the public communications network that is accessed via public access networks to a device subscribed to the communications network. The access to the service delivery element does not require the configuration functions described by Frailong.

Further, the present invention enables the ability of the claimed service delivery element, which is external to the network, to obtain a transport service for access to a network such as the Internet. It is a system that allows for automatic activation, authorization of transport privileges and upgrade of the data associated with the transport services. The service delivery element implements a secure interface to other service delivery elements to expand the services available to the subscriber. Accordingly, services can be added to the communications network using the claimed security delivery element so that it is transparent to a user, such as one practicing the invention disclosed by Frailong.

Moreover, Frailong's description of passwords, encryption keys, secure sockets layers and public key certificates are made in the context of upgrades or changes to parameters of the gateway interface device, downloads to the gateway interface device

and the relationship between the gateway interface device and the remote management server. See e.g. column 4, lines 55-59 ("The gateway interface device further provides connectivity to a remote server process which provides remote initialization, configuration, and upgrades of the gateway interface device without necessitating extensive interaction", column 17, lines 38-42 ("The reconfiguration protocol between the remote management server and the gateway interface device is used when the gateway interface device is to be reconfigured in some manner.") and column 18, line 26-29 ("The trust relationship between the gateway interface device and the remote management server is implemented through a comprehensive security framework provided by authentication and encryption mechanisms.") This is different than providing a secure interface between a feature server that is external to the communication network and the communication network. As required by the claims, this security interface and negotiated security level is provided by the service delivery element within the communication network. It is not provided by a combination of elements where one element is within the communication network and another element is outside the communication network. In addition, the discussion of security provided by Frailong concerns the two elements, i.e. the gateway interface device and the remote management server. The discussion does not touch on providing security for access to feature server for the communication network.

The claimed service delivery element implements a secure interface to expand the services available to the subscriber by providing a secure link to a feature server that is external to the communication network. Accordingly, services can be transparently added to the communications network from the user's perspective by using the claimed service delivery element and its secure external interface. The only examples Frailong provides regarding adding services investigate the configuration of a client device or upgrade the data of the client device. In order to accomplish these services, a user implementing Frailong's invention needs to implement the authentication methods to obtain transport access. Frailong, however, does not provide information on how to provide the secure access to the feature server as provided by the present invention.

In the June 5, 2007 Office Action and the November 29, 2007 Final Office Action, Willars is cited as overcoming Frailong's deficiencies in describing the claimed invention. Willars is cited to state that it is known to have a service delivery element with an internal interface. In other words, Willars is cited to suggest that it is know within the prior art to move Frailong's gateway identity device from being external to the network to being internal to the network. By combining Frailong and Willars it is suggested that the claimed invention is obvious. But as stated in the previous appeal and in Appellants' responses to the latest Office Actions, the claims include a service delivery element that is internal to the communication network, provides the security function within the communication network by negotiating a security level between the feature server and the communication network and provides a secure interface between the communication network and the external feature server. Citing a reference, i.e. Willars, to show that the service delivery element that is internal to the communication network is not sufficient to overcoming all the differences between Frailong and the claims.

Frailong's gateway interface device is not the only element disclosed by Frailong that is required to provide all the functionality required by the claimed service delivery element. Frailong also refers to the remote management server, which is separate from the gateway interface device and the client network, for teaching the security function found in the claims. The SSL is used by Frailong to work with at least the gateway interface device and the remote management server to provide the security features. Thus, by citing Willars and stating that Frailong's gateway interface device is internal to the network, the cited combination still relies on at least one element that is external to the network, the remote management server, to provide the security features. Moreover, the SSL is used to communication between the dispersed gateway interface and the remote management server to provide the security.

In the Response to Arguments section of the Final Office Action, citations are made to Willars that demonstrate that the features equivalent to the claimed service delivery element are actually within the communication network. Without admitting that Willars discloses that the service delivery element is within the communication element,

the cited sections, i.e. column 3. lines 61-65, column 4, lines 26-30 and lines 45-49 describe a multiplexer (MUX 33) multiplexing calls between core networks and a radio access network. Regardless these sections of Willars as well as the remainder of the reference do not describe the service delivery element having each of the claimed limitations including the embedded security layer that authenticates the feature server. Thus, Appellants respectfully submit that Willars does not provide the disclosure lacking in Frailong to describe the claimed invention. In other words, the mux does not provide all the features of the claimed service delivery element. Therefore, Willars and Frailong still distribute the features, which are claimed to be a part of the service delivery element and internal to the network, to be internal and external to the network.

It appears from the Response to Arguments section that Appellants' argument is simply that Willars does not disclose the service delivery element that is internal to communication network because no references to Willars having the service delivery element with the claimed features being within the communication network are found. Appellants' argument, however, is that Willars does not provide all the details necessary to overcome how Frailong does not disclose the claimed invention. As stated, Willars does not disclose these features, which are also not found in Frailong. The mere movement of Frailong's gateway interface device internally to the communication network does not also disclose the secure access to the feature services as required by the claims.

Appellants respectfully submit that the comments in the Advisory Action do not provide any additional information than what is provided in the June 5, 2007 Office Action and the November 29, 2007 Final Office Action. The Advisory Action still relies on Willars' mux to disclose the service delivery element being internal to the network. Willars' mux/, however, does not disclose the features of the remote management server being internal to the network. The Advisory Action relies on Frailong's SSL to state that the cited combination discloses all the features of the claimed embedded security layer. But Frailong's SSL works with Frailong's external remote management server and gateway identity device to provide the claimed embedded security layer. Thus,

Appellants respectfully submit that the combination of Frailong and Willars fails to disclose, teach or otherwise suggest each and every feature required by independent claims 1 and 22.

Appellants continue to assert that Frailong and Willars do not disclose, teach or otherwise suggest the service delivery element of the present invention having the embedded security layer. Frailong discloses the remote management server with contains security information such as passwords and encryption keys. Frailong and Willars do not embed these features into a security layer of the service delivery element even though Willars discloses the service delivery element being internal to the communication network. The claims provide for a unitary device within the network to provide secure access to a feature server that is external to the network thereby expanding the capabilities of the network, which is not disclosed by the cited combination.

(v) Conclusion

For the above reasons, the Appellants respectfully submit that the rejections of claims 1 and 22 under 35 U.S.C. §102(e) as being anticipated by Frailong are in error and should be reversed and the claims allowed. As claims 2-12 and 14-21 depend upon claim 1 and claims 23-38 depend upon claim 22 and include the limitations of independent claims, Appellants also submit that the rejection of these dependent claims are also patentable over Frailong.

8. CLAIMS APPENDIX

1. (Previously Amended) An apparatus for interfacing a communication network to a feature server external to the network, the apparatus comprising:

a service delivery element, wherein the service delivery element is within the communication network, the service delivery element comprising at least one internal interface to couple the service delivery element to other devices within the communication network, an external interface to couple the service delivery element to at least one feature server external to the communication network, an embedded security layer to authenticate the at least one feature server on the communication network and to provide a secure interface for the at least one feature server to the communication network through the external interface and a processor adapted to operate responsive to a control program stored within a memory associated with the processor; and wherein the service delivery element is operable to recognize the feature server, to negotiate a security level between the feature server and the communication network, and to manage access by the feature server to the communication network.

2. (Previously Amended) The apparatus of claim 1, wherein the security level defines a level of access of the feature server to the communication network.

3. (Previously Amended) The apparatus of claim 1, wherein, based upon the security level, the service delivery element restricts access by the feature server to at least one class of data retained within the communication network.

4. (Previously Amended) The apparatus of claim 1, wherein, based upon the security level, the service delivery element restricts access by the feature server to at least one internal function of the communication network.

5. (Previously Amended) The apparatus of claim 1, wherein based upon the security level, the service delivery element terminates access by the feature server.

6. (Previously Amended) The apparatus of claim 1, wherein the service delivery element provides scalable levels of access to the communication network by the feature server.

7. (Previously Amended) The apparatus of claim 1, wherein the service delivery element includes restriction criteria associated with varying degrees of authorization to the communication network by the feature server.

8. (Original) The apparatus of claim 7, wherein the restriction criteria comprises one of user based privileges and network operation variables.

9. (Original) The apparatus of claim 1, wherein the service delivery element is operable to provide one of access control, connectionless integrity, data origin authentication, replay packet rejection and confidentiality services.

10. (Original) The apparatus of claim 1, wherein the service delivery element includes a tunnel communication mode.

11. (Original) The apparatus of claim 10, wherein the tunnel communication mode comprises of an IP security protocol tunnel mode.

12. (Previously Amended) The apparatus of claim 1, wherein the service delivery element is configured to recognize a particular feature server.

13. (Cancelled)

14. (Previously Amended) The apparatus of claim 1, wherein the service delivery element establishes a security layer between the communication network and the feature server.

15. (Previously Amended) The apparatus of claim 1, wherein the service delivery element is operable to establish one of a static association and a dynamic association between the feature server and the communication network.

16. (Previously Amended) The apparatus of claim 1, wherein the service delivery element is operable to establish both a static association and a dynamic association between the feature server and the communication network at the same time.

17. (Previously Amended) The apparatus of claim 1, wherein the service delivery element is operable to provide an action responsive to the security level.

18. (Original) The apparatus of claim 17, wherein the action comprises one of creating a usage accounting record and providing a message.

19. (Previously Amended) The apparatus of claim 1, wherein the service delivery element is operable to expand access to the communication network by the feature server.

20. (Previously Amended) The apparatus of claim 19, wherein the service delivery element expands access to the communication network by the feature server subsequent to a renegotiation of the security level.

21. (Previously Amended) The apparatus of claim 1, wherein the service delivery element comprises a translation function.

22. (Previously Amended) A method of interfacing a communication network to a feature server external to the network comprising the steps of:

providing a service delivery element wherein the service delivery element being within the communication network and having an internal interface to couple the service delivery element to other elements within the communication network, an external

interface to couple the service delivery element to the feature server external to the network and an embedded security layer,

recognizing the feature server via the service delivery element,

authenticating the feature server for use on the communication network by the embedded security layer,

providing a secure interface for the at least one feature server to the communication network through the external interface by way of the embedded security layer;

negotiating a security level between the feature server and the communication network, and

metering access via the service delivery element by the feature server to the communication network in view of the security level.

23. (Previously Amended) The method of claim 22, wherein the security level defines a level of access of the feature server to the communication network.

24. (Previously Amended) The method of claim 22, wherein the method comprises, based upon the security level, restricting access by the feature server to at least one class of data retained within the communication network.

25. (Previously Amended) The method of claim 22, wherein the method comprises, based upon the security level, restricting access by the feature server to at least one internal function of the communication network.

26. (Previously Amended) The method of claim 22, wherein the method comprises, based upon the security level, terminating access to the communication network by the feature server.

27. (Previously Amended) The method of claim 22, further comprising scaling levels of access to the communication network by the feature server.

28. (Previously Amended) The method of claim 22, wherein the service delivery element includes restriction criteria, and wherein the method comprises varying degrees of authorization to the communication network by the feature server in view of the restriction criteria.

29. (Original) The method of claim 28, wherein the restriction criteria comprises one of user based privileges and network operation variables.

30. (Previously Amended) The method of claim 22, the method comprising tunneling data between the feature server and the communication network through the service delivery element.

31. (Previously Amended) The method of claim 22, wherein the step of recognizing ~~a~~ feature server comprises recognizing a particular feature server.

32. (Previously Amended) The method of claim 22, comprising establishing a security layer between the communication network and the feature server.

33. (Previously Amended) The method of claim 22, comprising establishing one of a static association and a dynamic association between the feature server and the communication network.

34. (Original) The method of claim 22, comprising, in response to a failure to negotiate a security level, providing an action responsive to the failure to negotiate a security level.

35. (Original) The method of claim 34, wherein the action comprises one of creating a usage accounting record, providing a recorded message and linking to a source of additional information.

36. (Previously Amended) The method of claim 22, comprising expanding access to the communication network by the feature server.

37. (Previously Amended) The method of claim 22, wherein the step of expanding access to the communication network by the feature server comprises renegotiating the security level.

38. (Previously Amended) The method of claim of claim 22, further comprising the step of translating data communicated between the feature server and the communication network.

9. EVIDENCE APPENDIX

No evidence has been submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132, nor has any other evidence been entered by the Examiner and relied upon by the Appellant.

10. RELATED PROCEEDINGS APPENDIX

The Appellant and Appellant's representative know of no other appeal, interference, or judicial proceeding that may be related to, directly affect or be directly affected by, or have a bearing upon the Board's decision in the pending appeal.

Please charge any fees associated herewith, including extension of time fees, to **50-2117**.

Respectfully submitted,
Banks, Robert et al..

SEND CORRESPONDENCE TO:

Motorola, Inc.
Law Department

Customer Number: **22917**

By: /Simon B. Anolick/

Simon B. Anolick
Attorney for Appellants
Registration No.: 37,585
Telephone: 847-576-4234
Fax: 847-576-3750